Jeff S. Westerman (SBN 94559)
ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
Telephone: (310) 752-9385
Facsimile: (877) 500-8781
Jeff.westerman@zimmreed.com

Brian C. Gudmundson (*Pro hac vice* forthcoming)
Michael J. Laird (*Pro hac vice* forthcoming)
Rachel K. Tack (*Pro hac vice* forthcoming)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

Rebecca Scifo, individually and on behalf of all others similarly situated,

Plaintiff,

v.

Carrington Mortgage Services, LLC & Alvaria, Inc.

Defendants.

CASE NO.: 8:23-CV-00805

COMPLAINT – CLASS ACTION

1. **Negligence**
2. **Negligence *Per Se***
3. **Violation of the California Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq*.**
4. **Violation of the California Civil Code § 1798.150**
5. **Declaratory and Injunctive Relief**

(Jury Trial Demanded)

Plaintiff Rebecca Scifo ("Plaintiff"), by her undersigned counsel, files this Class Action Complaint on behalf of herself and a class of similarly situated persons against Alvaria, Inc. ("Alvaria") and Carrington Mortgage Services, LLC ("Carrington") (collectively "Defendants"). Plaintiff bases the forgoing allegations upon personal information and belief, the investigation of counsel, and states the following:

INTRODUCTION

1. Alvaria is a workforce management and call center technology solution company. It provides these services to Carrington, which is the current owner of Plaintiff's home mortgage.

2. On March 9, 2023, third party hackers breached Alvaria's data system, including a portion of Alvaria's customer environment that maintained customer's workforce management and/or outbound dialer data ("Data Breach"). Some of the data the hackers procured or exfiltrated was associated with Carrington and included Plaintiff's data.

3. This is the second security incident at Alvaria in four months. Last November, the company suffered a hack by the Hive Ransomware group. That incident impacted nearly 5,000 customers.[1]

4. The types of data impacted by the Data Breach included names, mailing addresses, telephone numbers, loan numbers, current loan balances, and the last four digits of Social Security Numbers. Neither Carrington nor Alvaria have disclosed the total number of customers and clients impacted by the Data Breach. However, Alvaria did report to the Massachusetts Attorney General that at least 4,167 Massachusetts residents were impacted by the Data Breach.[2]

---

[1] *Tech vendor names Carrington in data breach notice*, NEXT, May 3, 2023, https://nextmortgagenews.com/news/tech-vendor-names-carrington-in-data-breach-notice/ (last visited May 5, 2023).

[2] Andrew Martinez, *Carrington Reports Ransomware Attack at Tech Vendor*, NATIONAL MORTGAGE NEWS, May 2, 2023,

5. Because the Data Breach compromised Plaintiff's Sensitive Information, Plaintiff and the Class (defined below) have been placed in an immediate and continuing risk of harm from fraud, identity theft, and related harm caused by the Data Breach.

6. As a result of Defendants' conduct, Plaintiff and the Class have and will be required to continue to undertake time-consuming and often costly efforts to mitigate the actual and potential harm caused by the Data Breach. This includes efforts to mitigate the breach's exposure of their Sensitive Information, including by, among other things, placing freezes and setting alerts with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, reviewing and monitoring credit reports and accounts for unauthorized activity, changing passwords on potentially impacted websites and applications, and requesting and maintaining accurate medical records.

7. Plaintiff therefore brings this Class Action seeking relief for her injuries and those of persons who were similarly impacted by the Data Breach and Defendants' inadequate data security.

JURISDICTION

8. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005. Subject matter jurisdiction is proper because: (1) the amount in controversy in this class action exceeds five million dollars ($5,000,000), excluding interest and costs; (2) there are more than 100 Class members; (3) at least one member of the Class is diverse from the Defendants; and (4) the Defendants are not a government entity.

9. This Court has general personal jurisdiction over Carrington because Carrington is a resident of the State of California, it has a registered corporate office in Glendale, California, and it has its principal address in Anaheim, California. Alvaria is

---

https://www.nationalmortgagenews.com/news/carrington-mortgage-reports-ransomware-data-breach (last visited May 5, 2023).

a resident of Westford, Massachusetts and has sufficient minimum contacts with California to establish specific personal jurisdiction because it contracted with Carrington, which is headquartered in California, to provide data security services to Carrington's customers (the reasonableness and adequacy of the data security related to the service Alvaria provided to Carrington is directly at issue in this litigation), including Plaintiff, and Alvaria conducts substantial business in California.

10. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in California and because Defendants conduct a substantial part of their business within this District.

PARTIES

11. **Plaintiff** Rebecca Scifo is and has been for all relevant times a resident of Chancellor, South Dakota and is a citizen of South Dakota. Carrington currently owns Ms. Scifo's home mortgage and has owned her mortgage for approximately the last five years. Ms. Scifo received a notice letter from Alvaria on May 2, 2023, indicating that her data, including her name, mailing address, telephone number, loan number, current loan balance, and the last four digits of her Social Security Number had been implicated in Alvaria's March 9, 2023 data breach. The notice Ms. Scifo received from Alvaria ("Notice") is attached hereto as Exhibit A. Since notice of the Data Breach, Plaintiff has spent time and effort monitoring her accounts for identity theft or fraud.

12. **Defendant** Carrington is a limited liability company formed in Delaware with its principal and mailing address located in Anaheim, California. Carrington's registered agent is 1505 Corporation C T Corporation System, located at 330 N. Brand Blvd, Glendale, California.

13. **Defendant** Alvaria is a corporation with its headquarters and principal place of business at 5 Technology Park Drive, Westford, Massachusetts, 01886. Alvaria also has a registered agent in California, CSC—Lawyers Incorporating Service, located at 2710 Gateway Oaks Dr. Ste. 150 N, Sacramento, California, 95833.

BACKGROUND

A. Defendants Collected, Maintained, and Stored Sensitive Information.

Carrington

14. In providing its loan and financial services, Carrington collects sensitive personal information from customers. This information includes name, email address, username, password, social security number, phone number, mailing address, financial information and history, employment information drivers' license information, insurance information, marital status, and other personal and highly sensitive information a person might provide when trying to procure a loan or mortgage. Carrington hosts a large repository of sensitive personal information for its customers. Carrington also contracts with Alvaria for certain call center related services, by which Carrington authorizes Alvaria to receive and store Carrington's customers' data.

Alvaria

15. Alvaria claims to be the "world leader in enterprise-scale customer experience and workforce engagement management." It states that it is a "technology innovator[] in call center software, cloud contact center solutions, workforce optimization and customer service experience."[3]

16. According to Alvaria, it serves 4 of 5 top commercial banks, 8 of 10 top telecom providers, 6 of 6 top airline carriers, 4 of 5 top healthcare providers, and 4 of 5 top general merchandisers.[4]

17. In providing its services, Alvaria collects information from its clients, including Carrington, that may include sensitive information like name, mailing address, social security numbers, loan information, and other related information that customers provided directly to Carrington.

[3] https://www.linkedin.com/company/alvaria-inc.

[4] https://www.alvaria.com/company/about-alvaria.

B. Defendants Knew They Needed to Protect Customers' Sensitive Information and Committed to Protecting that Information.

Carrington

18. Carrington has a Privacy Policy on its website that states that it respects "the privacy of each user."[5]

19. Carrington also makes other representations related to customer privacy including:

(1) Ensuring the privacy of [customer] confidential information is one of Carrington Mortgage Services, LLC's top priorities;

(2) We comply with all applicable federal, state, and local laws, and have numerous internal safeguards in place to protect your personal information. Carrington Mortgage Services, LLC's Privacy Officer oversees all aspects of our privacy policy throughout the company. We treat confidential customer information with the utmost discretion and caution, and we hold our business partners (presumably like Alvaria) to these same high standards.[6]

20. Carrington knew it needed to protect the privacy of Plaintiff and the Class and further committed to holding its partners, like Alvaria, to the very same privacy protection standards it follows.

Alvaria

21. Alvaria's Privacy Policy commits to "keeping [customers] personal information confidential and secure." The Policy further explains that Alvaria maintains "appropriate physical, electronic, procedural, technical and organizational measures to help safeguard person information from loss, theft, misuse, unauthorized access, disclosure, alteration and destruction."[7]

---

[5] https://www.carringtonmortgage.com/legal/privacy-policy.

[6] https://www.carringtonmortgage.com/legal/best-practices#protectingPrivacy.

[7] https://www.alvaria.com/legal/privacy-policy.

22. Alvaria knew the information from Carrington customers was highly sensitive and that it was required by law to maintain the privacy and confidentiality of that information.

C. Defendants' Inadequate Data Security Measures Exposed Customers' Sensitive Information.

23. On March 9, 2023, a malicious actor gained unauthorized access to Alvaria's data systems, which included customer databases. By doing so, the actor gained access to the sensitive personal, financial, and other information of Carrington's clients' current and former customers.

24. Upon information and belief, the actors viewed, copied, and exfiltrated substantial amounts of Plaintiff's and the Class's PII. This included highly sensitive information such as names, mailing addresses, loan information, and partial Social Security Numbers.

25. This is not Alvaria's first data breach. In November of 2022, Alvaria's data system was breached, but that instance was purportedly limited to disclosure of certain corporate clients' information. Upon information and belief, Carrington was aware of the November 2022 breach of Alvaria's data systems.

26. Neither Alvaria nor Carrington immediately disclosed this new March 2023 Data Breach to the victims impacted by the unauthorized disclosure. Rather, Alvaria waited until April 26, 2023 to publicly post notice of the breach, approximately seven weeks after it learned of the Data Breach. Additionally, neither of the Defendants have disclosed the scope of the breach or the total number of impacted consumers.

27. The April 26, 2023 notice that Alvaria provided to Plaintiff and the Class members suggested they take time consuming steps to help protect their information, including enrolling in identity monitoring services, obtaining a free credit report, setting up fraud alerts, and issuing a security freeze.

28. Given that Defendants purposefully obtained and stored the PII of Plaintiff and the Class and knew or should have known of the serious risk and harm caused by a

data breach, Defendants were obligated to implement reasonable measures to prevent and detect cyberattacks. This includes measures recommended by the Federal Trade Commission and promoted by data security experts and other agencies. This obligation stems from the foreseeable risk of a data breach given that Defendants collected, stored, and had access to a swath of highly sensitive patient records and data and, additionally, because other highly publicized data breaches at different institutions put Defendants on notice that the highly personal data they stored, or allowed other entities to store via a services contract or relationship, might be targeted by cybercriminals.

29. Despite the highly sensitive nature of the information Defendants obtained, created, and stored, and the prevalence of data breaches at financial institutions like Carrington or related businesses, Defendants inexplicably failed to take appropriate steps to safeguard the PII of Plaintiff and the Class. The Data Breach itself and information Defendants have disclosed about the breach to date, including its length, the need to remediate Defendants' cybersecurity, and the sensitive nature of the impacted data, collectively demonstrate Defendants failed to implement reasonable measures to prevent the Data Breach and the exposure of highly sensitive customer information.

D. Exposure of PII and other Sensitive Information Created a Substantial Risk of Harm.

30. The personal and financial information of Plaintiff and the Class is valuable and has become a highly desirable commodity to data thieves.

31. Defendants' failure to reasonably safeguard Plaintiff's and the Class's sensitive PII has created a serious risk to Plaintiff and the Class, including both a short-term and long-term risk of identity theft and other fraud.

32. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

33. According to experts, one out of four data breach notification recipients

becomes a victim of identity fraud.[8]

34. Stolen Sensitive Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines and is frequented by criminals, fraudsters, and other wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal identities and online activity.

35. Purchasers of Sensitive Information use it to gain access to the victim's bank accounts, social media, credit cards, and tax details. This can result in the discovery and release of additional Sensitive Information from the victim, as well as Sensitive Information from family, friends, and colleagues of the original victim. Victims of identity theft can also suffer emotional distress, blackmail, or other forms of harassment in person or online. Losses encompass financial data and tangible money, along with unreported emotional harms.

36. The FBI's Internet Crime Complaint (IC3) 2019 report estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone. The same report identified "rapid reporting" as a tool to help stop fraudulent transactions and mitigate losses.

37. Defendant did not rapidly report to Plaintiff and the Class that their Sensitive Information had been exposed or stolen, but instead seven weeks to make a public notice related to the Data Breach, and even that notice did not include the number of impacted victims.

38. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour reiterated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their

[8] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims,* ThreatPost.com (last visited Jan. 17, 2022), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/.

information may be commercially valuable. Data is currency."[9]

39. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require:

(1) encrypting information stored on computer networks;

(2) retaining payment card information only as long as necessary;

(3) properly disposing of personal information that is no longer needed or can be disposed of pursuant to relevant state and federal laws;

(4) limiting administrative access to business systems;

(5) using industry tested and accepted methods;

(6) monitoring activity on networks to uncover unapproved activity;

(7) verifying that privacy and security features function properly;

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.[10]

40. The United States Cybersecurity & Infrastructure Security Agency, and other federal agencies, recommend similar and supplemental measures to prevent and detect cyberattacks, including, but not limited to: implementing an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring firewalls, automating anti-virus and anti-malware programs, managing privileged accounts, configuring access controls, disabling remote desktop protocol, and updating and patching computers.

41. The FTC cautions businesses that failure to protect Sensitive Information and the resulting data breaches can destroy consumers' finances, credit history, and

[9] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited June 7, 2022) https://www.ftc.gov/news-events/news/speeches/remarks-ftc-exploring-privacy-roundtable.

[10] *Start With Security, A Guide for Business,* FTC (last visited June 7, 2022) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

reputations, and can take time, money, and patience to resolve the fallout.[11] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures—like Defendants failed to do here—as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

E. Plaintiff and the Class's PII are Valuable.

42. Birth dates, Social Security numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on an ongoing basis rather than exploiting just one account until it's canceled.[12]

43. For that reason, cybercriminals on the dark web are able to sell data like Social Security numbers for large profits.

44. Consumers place a considerable value on their Sensitive Information and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth between $30.49 and $44.62.[13] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

45. Defendant's Data Breach exposed a variety of Sensitive Information, including Social Security numbers and PII.

46. The Social Security Administration ("SSA") warns that a stolen Social

[11] Taking Charge, What to Do if Your Identity is Stolen, FTC (last visited June 7, 2022), https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0014-identity-theft.pdf.

[12] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers,* Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 7, 2022).

[13] 11-Horn Hann, Kai-Lung Hui, et al, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited June 7, 2022).

Security number can lead to identity theft and fraud: "Identity thieves can use your number and your credit to apply for more credit in your name."[14] If the identity thief applies for credit and does not pay the bill, it will damage victims' credit and cause a series of other related problems.

47. Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

48. Plaintiff and the Class now face years of monitoring their financial and personal records with a high degree of scrutiny. The Class has incurred and will incur this damage in addition to any fraudulent use of their Sensitive Information.

CLASS ALLEGATIONS

49. Plaintiff brings this action on behalf of himself and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class:

> All individuals whose data was impacted or otherwise compromised by the Data Breach.

50. Excluded from the class is Defendants and their subsidiaries and affiliates; all persons who make a timely election to be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

51. Plaintiff reserves the right to, after conducting discovery, modify, expand or amend the above Class definition or to seek certification of a class or Classes defined differently than above before any court determines whether certification is appropriate.

52. Numerosity. Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is

[14] Social Security Administration, Identity Theft and Your Social Security Number, (last visited June 7, 2022), https://www.ssa.gov/pubs/EN-05-10064.pdf.

impracticable. Plaintiff believes that there are thousands of members of the Class, if not more. The number of impacted individuals remains unknown and unreported, and Plaintiff believes additional entities and persons may have been affected by the Data Breach. The precise number of class members, however, is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

53. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether Defendants knew or should have known that their data environment and cybersecurity measures, or those created by corporate service providers, created a risk of a data breach;

b. Whether Defendants controlled and took responsibility for protecting Plaintiff's and the Class's data when they solicited that data, collected it, stored it on its servers, and authorized a third party to collect and store that data;

c. Whether Defendants' security measures were reasonable considering the FTC data security recommendations, state laws and guidelines, industry standards, and common recommendations made by data security experts;

d. Whether Defendants owed Plaintiff and the Class a duty to implement reasonable security measures;

e. Whether Defendants' failure to adequately secure Plaintiff's and the Class's data constitutes a breach of its duty to institute reasonable security measures;

f. Whether Defendants' failure to implement reasonable data security measures allowed the breach of their data systems to occur and caused the theft of Plaintiff's and the Class's data;

g. Whether reasonable security measures known and recommended by the data security community could have prevented the breach;

h. Whether Plaintiff and the Class were injured and suffered damages or other losses because of Defendants' failure to reasonably protect its data systems; and

i. Whether Plaintiff and the Class are entitled to relief.

54. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff is a typical member of the Class. Plaintiff and the Class are each persons whose provided data to Carrington, whose data resided on Carrington's and Alvaria's servers, and whose personally identifying information was exposed in Defendants' Data Breach. Plaintiff's injuries are similar to other class members and Plaintiff seeks relief consistent with the relief due to the Class.

55. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Defendants to obtain relief for himself and for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated data breach cases. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

56. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit customers to recover even if their damages are small as compared to the burden and

expense of litigation, a quintessential purpose of the class action mechanism.

57. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), Defendants, through their conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

LEGAL CLAIMS

COUNT I

Negligence

58. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

59. Defendants' owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the sensitive data it solicited from Plaintiff and the Class and managed and stored. This duty arises from multiple sources.

60. Defendants owed a common law duty to Plaintiff and the Class to implement reasonable data security measures because it was foreseeable that hackers would target Defendants' data systems and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and the Class would be harmed. Defendants controlled their technology, infrastructure, and cybersecurity, and to the extent Carrington outsourced its data security to Alvaria, Carrington made the decision to outsource that service.

61. Defendants further knew or should have known that if hackers breached their data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. Furthermore, Defendants knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and the Class, was the foreseeable consequence of Defendants' unsecured, unreasonable data security measures.

62. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15

U.S.C. § 45, required Defendants to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Defendants' duty to Plaintiff and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendants failing to use reasonable measures to protect sensitive data. Defendants, therefore, were required and obligated to take reasonable measures to protect data they possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendants' duty to adequately protect sensitive information. By failing to implement reasonable data security measures, Defendants' acted in violation of § 5 of the FTCA.

63. Defendants are obligated to perform their business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Defendants to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

64. Finally, Defendants assumed the duty to protect sensitive data by soliciting, collecting, and storing users' data and, additionally, by representing to consumers that it lawfully complied with data security requirements and had adequate data security measures in place to protect the confidentiality of Plaintiff's and the Class's private and sensitive information.

65. Defendants breached their duty to Plaintiff and the Class by implementing unreasonable data security measures that they knew or should have known could cause a Data Breach. Defendants knew or should have known that hackers might target sensitive data that Carrington solicited and collected, which was later collected and stored by Alvaria, on customers and, therefore, needed to use reasonable data security measures to protect against a Data Breach. Indeed, Defendants acknowledged they were subject to certain standards to protect data and utilize other industry standard data security measures.

66. Defendants were fully capable of preventing the Data Breach. Alvaria, as a technology utilizing company, and Carrington, a massive and savvy financial entity, knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach. Defendants thus failed to take reasonable measures to secure its system, leaving it vulnerable to a breach.

67. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

COUNT II

Negligence Per Se

68. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

69. Defendants' unreasonable data security measures and constitute unfair or deceptive acts or practices in or affecting commerce in violation Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, both require businesses to institute reasonable data security measures and breach notification procedures, which Defendants failed to do.

70. Section 5 of the FTCA, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendants of failing to use reasonable measures to protect users' sensitive data. The FTC's complaint against Defendants also forms the basis of Defendants' duty.

71. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect users' personally identifying information and sensitive data and by not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the sensitive nature and amount of data is stored on their users and

the foreseeable consequences of a Data Breach should Defendants fail to secure their systems.

72. Defendants' violation of Section 5 of the FTC Act constitutes negligence per se.

73. Plaintiff and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) was intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class.

74. As a direct and proximate result of Defendants' negligence per se, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT III

Violation of the California Legal Remedies Act,

Cal. Civ. Code §§ 1750, *et seq.*

75. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

76. The Consumers Legal Remedies Act ("CLRA") is liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

77. Defendants are each a "person" as defined by the CLRA, and both provided "services" as defined under the act. Cal. Civ. Code §§ 1761(b)-(c), 1770.

78. The CLRA prohibits a defendant who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have." *Id*. at § 1770(a)(5).

79. Additionally, the CLRA prohibits a defendant who is involved in a

transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another." *Id*. at § 1770(a)(7).

80. Plaintiff and the Class members are "consumer[s]" as who were engaged in a "transaction" under the act. *Id*. at §§ 1761(d)-(e), 1770.

81. Defendants acts and practices were intended to and did result in providing services to Plaintiff and the California Class members in violation of Civil Code § 1770, including, but not limited to, the following:

a. Implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient to protect Plaintiff's and the Class's sensitive data, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Class members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's Class members' sensitive data; and

e. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Class members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

82. Defendants' omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' sensitive information that Defendants

solicited, collected, and stored.

83. Had Defendants disclosed, rather than concealing, to Plaintiff and Class members that their cybersecurity, digital platforms, and data storage systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

84. Instead, Defendants received, maintained, and compiled Plaintiff's and Class members' sensitive data as part of the services Defendants provided and for which Plaintiff and Class members paid, in part, through transaction fees by (1) omitting and concealing information from Plaintiff and Class members that Defendants' data security practices were knowingly insufficient to maintain the safety and confidentiality of Plaintiff's and Class members' sensitive data and (2) that Defendants was not compliant with basic data security requirements and best practices to prevent a Data Breach. Accordingly, Plaintiff Class members acted reasonably in relying on Defendants' omissions, the truth of which they could not have discovered.

85. On May 8, 2023, Plaintiff and the proposed Class provided notice of their claims for damages to Defendants in compliance with California Civil Code § 1782(a) via certified mail. Plaintiff and the other members of the Class seek only injunctive relief in this complaint, but will amend this complaint to seek damages if Defendants do not comply with the California Civil Code § 1782(a) notice.

COUNT IV

Violation of the California Consumer Privacy Act

Civil Code § 1798.150

86. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

87. Defendant Carrington is a corporation organized or operated for the profit or financial benefit of its owners.

88. Defendant Alvaria is a corporation organized or operated for the profit or

financial benefit of its owners.

89. Defendants collect and stores consumers personal information, including sensitive and personal information, as defined by Cal. Civ. Code §1798.150 and § 1798.81.5 therein. Defendant Carrington individually collects and stores consumers data and it also hired Alvaria for some services and in turn, Alvaria received some of Carrington's customers' personal and private information. Both Carrington and Alvaria represent to consumers that they will keep consumers' private information private and confidential.

90. Defendants had a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and members of the Class's sensitive and personal data.

91. Defendants failed to meet their duty, resulting in unauthorized access and exfiltration, theft, or disclose of Plaintiff's and the Class's, personal and sensitive data in violation of § 1798.150.

92. Plaintiff and members of the Class seek relief pursuant to § 1798.150(a) and Cal. Code Civ. Proc. § 1021.5 including *inter alia*, actual damages, injunctive relief, attorneys' fees and costs, and any other relief this Court deems proper.

93. Because Defendants are still in possession of Plaintiff's and the Class's, sensitive and personal data, Plaintiff seeks injunctive or other equitable relief to ensure that Defendants implement and maintain reasonable data security measures and practices to prevent an event like the Data Breach from occurring again.

94. On May 8, 2023, Plaintiff and the proposed Class sent Defendants notice pursuant to § 1798.150(b) via certified mail. Plaintiff and the other members of the Class seek only injunctive relief pursuant to this count at this time, but will amend this complaint to seek damages if Defendants do not comply with the California Civil Code § 171798.150(b) notice.

COUNT V

Declaratory and Injunctive Relief

95. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

96. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

97. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendants' common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges Defendants' actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

98. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed, and continue to owe a legal duty to secure the sensitive information with which they are entrusted, specifically including information obtained from its customers, and to notify impacted individuals of the Data Breach under the common law, Section 5 of the FTC Act;

b. Defendants breached, and continue to breach, their legal duty by failing to employ reasonable measures to secure their customers' personal information; and,

c. Defendants' breach of their legal duty continues to cause harm to Plaintiff and the Class.

99. The Court should also issue corresponding injunctive relief requiring

Defendants to employ adequate security protocols consistent with industry standards to protect its users' data.

100. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendants' data systems. If another breach of Defendants' data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

101. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued.

102. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

103. Wherefore, Plaintiff, on behalf of herself and the Class, requests that this Court award relief as follows:

a. An order certifying the class and designating Plaintiff as the Class Representative and her counsel as Class Counsel;

b. An award to Plaintiff and the proposed Class members of damages with pre-judgment and post-judgment interest;

c. A declaratory judgment in favor of Plaintiff and the Class;

d. Injunctive relief to Plaintiff and the Class;

e. An award of attorneys' fees and costs as allowed by law; and

f. An award such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

Plaintiff hereby demands a jury trial for all the claims so triable.

Respectfully submitted,

Dated: May 8, 2023

/s/ Jeff S. Westerman
Jeff Westerman
ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
Telephone: (310) 752-9385
Facsimile: (877) 500-8781
Jeff.westerman@zimmreed.com

Brian C. Gudmundson
(*Pro hac vice* forthcoming)
Michael J. Laird
(*Pro hac vice* forthcoming)
Rachel K. Tack
(*Pro hac vice* forthcoming)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Attorneys for Plaintiff and the Proposed Class

EXHIBIT A

ALVARIA®

Return Mail Processing
PO Box 999
Suwanee, GA 30024

268 1 89721 **********AUTO**ALL FOR AADC 570
REBECCA SCIFO
530 2ND ST
CHANCELLOR, SD 57015-2003

April 26, 2023

Re: Notice of Data Incident

Dear Rebecca Scifo:

Alvaria, Inc. ("Alvaria") is a workforce management and call center technology solution company. We write to inform you about a recent incident experienced by Alvaria that may have involved some of your personal information, which came into our possession due to the services we provide Carrington Mortgage Services, LLC. We are providing you with information about the incident and steps you can take to protect yourself, should you feel it necessary to do so.

What Happened? On March 9, 2023, Alvaria was the victim of a sophisticated ransomware attack on a portion of our customer environment that maintained some of our customers' workforce management and/or outbound dialer data. Upon discovery, we immediately secured our networks, safely restored our systems and operations via viable backups, and initiated an investigation of the incident with the assistance of forensic experts. Our investigation determined that, on March 9, 2023, the unauthorized actor obtained access to and procured some data associated with Carrington Mortgage Services, LLC, which may have contained your personal information. Presently, we have no evidence of actual or attempted misuse of your personal information.

What Information Was Involved. The impacted files may have contained your personal information, including your name, mailing address, telephone number, loan number, current loan balance, and the last four digits of your Social Security number.

What We Are Doing. Upon discovery of the incident, we immediately secured our networks, implemented measures to further improve the security of our systems, safely restored our systems and operations via viable backups, initiated an investigation of the incident with the assistance of forensic experts, and notified the Federal Bureau of Investigation ("FBI"). We also are notifying you so that you may take further steps to protect your information, should you feel it appropriate to do so. In addition, we are providing you with access to 24 months of credit monitoring and identity restoration services through Experian at no charge to you. You must enroll by July 31, 2023.

What You Can Do. Please review the enclosed "*Steps You can take to Help Protect Your Information*" which describes the services we are offering, how to activate them, and provides further details on how to protect yourself. We encourage you to remain vigilant against the potential for identity theft and fraud and to monitor your accounts and credit reports for any suspicious activity.

For More Information. We sincerely regret any inconvenience this incident may have caused you. If you have additional questions, you may call our dedicated assistance line (800) 984-8166 (toll-free), Monday–Friday, from 9:00 a.m. to 11:00 p.m. Eastern Time, and Saturday–Sunday, 11:00 a.m. to 8:00 p.m. Eastern Time. Please be prepared to provide engagement number B090604.

Sincerely,

Jacques Greyling
Chief Operations Officer

Engagement # B090604

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Complimentary Identity Monitoring Services

We are providing you with a 24-month membership of Experian's IdentityWorks. A credit card is not required for enrollment in the identity monitoring services. To enroll, at no cost to you,

- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **MSK5N3MJ9**
- Ensure that you **enroll by**: **July 31, 2023** (Your code will not work after this date.)

With Experian IdentityWorks, you can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. Offline members may call for additional reports quarterly.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (800) 984-8166 by **July 31, 2023**. Be prepared to provide engagement number **B090604** as proof of eligibility for the identity restoration services by Experian.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (800) 984-8166. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Free Credit Report

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus (Equifax, Experian, and TransUnion). Obtaining a copy of your credit report from each agency on an annual basis, and reviewing it for suspicious activity, can help you spot problems and address them quickly. You can request your free credit report online at www.annualcreditreport.com or by phone at 1-877-322-8228. You can also request your free credit report by completing the request form at: www.annualcreditreport.com, and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Fraud Alert

As a precaution against identity theft, you can consider placing a fraud alert on your credit file. A "fraud alert" tells creditors to contact you before opening a new account or changing an existing account. A fraud alert also lets your creditors know to watch for unusual or suspicious activity. To place a fraud alert, call any one of the three major credit reporting agencies listed below. An initial fraud alert remains effective for ninety days, and is free of charge. If you wish, you can renew the fraud alert at the expiration of this initial period. As soon as one credit agency confirms your fraud alert, the others are notified to place fraud alerts on your file.

Equifax®
P.O. Box 105069
Atlanta, GA 30348-5069
1-800-685-1111
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion®
P.O. Box 2000
Chester, PA 19016-1000
1-800-916-8800
https://www.transunion.com/fraud-alerts

Security Freeze

Under the law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Federal law also allows consumers to place, lift or remove a security freeze on their credit reports at no charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

To place a security freeze on your credit report, you must send a written request by regular, certified, or overnight mail at the addresses below to *each* of the three major credit reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). You may also request the security freeze through *each* of the credit reporting agencies' websites or over the phone:

Equifax®
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045
https://www.equifax.com/personal/help/place-lift-remove-security-freeze/

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion®
P.O. Box 160
Woodlyn, PA 19094
1-800-916-8800
www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Additional Information

You may obtain additional information about identity theft (including, a security freeze) by contacting the above, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

For District of Columbia residents, the Attorney General may be contacted at: 400 6th Street NW, Washington, DC 20001; 202-727-3400; or oag@dc.gov.

For Maryland residents, the Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 410-528-8662; 1-888-743-0023; or https://www.marylandattorneygeneral.gov.

For New York residents, more information about steps to take to avoid identify theft can be obtained by contacting the New York State Attorney General (https://ag.ny.gov/internet/data-breach; 1-800-788-9898), the New York State Department of State's Division of Consumer Protection (https://dos.ny.gov/consumer-protection; 1-800-697-1220), or the New York State Division of State Police (1-800-342-3619; https://www.ny.gov/agencies/division-state-police).

For North Carolina residents, the Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island residents, the Attorney General may be contacted at 150 South Main Street, Provident RI 02903; 401-274-440; or www.riag.ri.gov.